United Nations A/CN.9/608/Add.2

General Assembly

Distr.: General
22 March 2006

Original: English

United Nations Commission on International Trade Law
Thirty-ninth session
New York, 19 June-7 July 2006

Legal aspects of electronic commerce

Explanatory Note on the Convention on the Use of Electronic Communications in International Contracts

Note by the Secretariat

Addendum

1. The Commission approved the final draft of the United Nations Convention on the Use of Electronic Communications in International Contracts ("the Convention") at its thirty-eighth session (Vienna, 4-15 July 2005). The Convention was subsequently adopted by the General Assembly on 23 November 2005 and opened it for signature from 16 January 2006 to 16 January 2008.

2. When it approved the final draft for adoption by the General Assembly, at its thirty-eighth session, the Commission requested the Secretariat to prepare explanatory notes on the Convention and present them to the Commission at its thirty-ninth session (see A/60/17, para. 165).

3. Annex I to this note contains article-by-article remarks on the Convention. The Commission may wish to take note of the explanatory notes and request their publication by the Secretariat, together with the final text of the Convention.

V.06-52316 (E) 040506 040506

IV. Article-by-article remarks (*continued*)

CHAPTER III. USE OF ELECTRONIC COMMUNICATIONS IN INTERNATIONAL CONTRACTS

Article 8. Legal recognition of electronic communications

1. A communication or a contract shall not be denied validity or enforceability on the sole ground that it is in the form of an electronic communication.

2. Nothing in this Convention requires a party to use or accept electronic communications, but a party's agreement to do so may be inferred from the party's conduct.

1. Non-discrimination of electronic communications

1. Paragraph 1 of this article restates the general principle of non-discrimination that is contained in article 5 of the UNCITRAL Model Law on Electronic Commerce. This provision means that there should be no disparity of treatment between electronic communications and paper documents, but is not intended to override any of the requirements contained in article 9. By stating that "information shall not be denied validity or enforceability solely on the grounds that it is in the form of an electronic communication", article 8, paragraph 1, merely indicates that the form in which certain information is presented or retained cannot be used as the only reason for which that information would be denied legal effectiveness, validity or enforceability. However, this provision should not be misinterpreted as establishing the absolute legal validity of any given electronic communication or of any information contained therein (A/CN.9/546, para. 41).

2. No specific rule has been included in the Convention on the time and place of formation of contracts in cases where an offer or the acceptance of an offer is expressed by means of electronic communications message, in order not to interfere with national law applicable to contract formation. UNCITRAL was of the view that such a provision would exceed the aim of the Convention, which is limited to providing that electronic communications would achieve the same degree of legal certainty as paper-based communications. The combination of existing rules on the formation of contracts with the provisions contained in article 10 is designed to dispel uncertainty as to the time and place of formation of contracts in cases where the offer or the acceptance are exchanged electronically (see below, paras. 43-64).

2. Consent to use electronic communications

3. Provisions similar to paragraph 2 have been included in a number of national laws relating to electronic commerce to highlight the principle of party autonomy and make it clear that the legal recognition of electronic communications does not require a party to use or accept them (A/60/17, para. 52; see also A/CN.9/527, para. 108).

4. However, the consent to use electronic communications does not need to be expressly indicated or be given in any particular form. While absolute certainty can be accomplished by obtaining an explicit contract before relying on electronic communications, such an explicit contract should not be necessary. Indeed, such a requirement would itself be an unreasonable barrier to electronic commerce. Under the Convention, the consent to use electronic communications is to be found from all circumstances, including the parties' conduct. Examples of circumstances from which it may be found that a party has agreed to conduct transactions electronically include the following: handing out a business card with a business e-mail address; inviting a potential client to visit a company's website or accessing someone's website to place an order; advertising goods over the Internet or through e-mail.

References to preparatory work:

UNCITRAL, 38th session (Vienna, 4-15 July 2005)	A/60/17, paras. 51-53
WG.IV, 44th session (Vienna, 11-22 October 2004)	A/CN.9/571, paras. 117-122
WG.IV, 42nd session (Vienna, 17-21 November 2003)	A/CN.9/546, paras. 44-45
WG.IV, 41st session (New York, 5-9 May 2003)	A/CN.9/528, paras. 94-108; see also paras. 121-131 (on related draft provisions since deleted)
WG.IV, 39th session (New York, 11-15 March 2002)	A/CN.9/509, paras. 86-92; see also paras. 66-73 (on related draft provisions since deleted)

Article 9. Form requirements

1. Nothing in this Convention requires a communication or a contract to be made or evidenced in any particular form.

2. Where the law requires that a communication or a contract should be in writing, or provides consequences for the absence of a writing, that requirement is met by an electronic communication if the information contained therein is accessible so as to be usable for subsequent reference.

3. Where the law requires that a communication or a contract should be signed by a party, or provides consequences for the absence of a signature, that requirement is met in relation to an electronic communication if:

(a) A method is used to identify the party and to indicate that party's intention in respect of the information contained in the electronic communication; and

(b) The method used is either:

(i) As reliable as appropriate for the purpose for which the electronic communication was generated or communicated, in

the light of all the circumstances, including any relevant agreement; or

(ii) Proven in fact to have fulfilled the functions described in subparagraph (a) above, by itself or together with further evidence.

4. Where the law requires that a communication or a contract should be made available or retained in its original form, or provides consequences for the absence of an original, that requirement is met in relation to an electronic communication if:

(a) There exists a reliable assurance as to the integrity of the information it contains from the time when it was first generated in its final form, as an electronic communication or otherwise; and

(b) Where it is required that the information it contains be made available, that information is capable of being displayed to the person to whom it is to be made available.

5. For the purposes of paragraph 4 (a):

(a) The criteria for assessing integrity shall be whether the information has remained complete and unaltered, apart from the addition of any endorsement and any change which arises in the normal course of communication, storage and display; and

(b) The standard of reliability required shall be assessed in the light of the purpose for which the information was generated and in the light of all the relevant circumstances.

1. General remarks

5. Like the UNCITRAL Model Law on Electronic commerce, on which it is based, the Convention relies on what has become known as the "functional equivalence approach" (see A/CN.9/608/Add.1, paras. 7-9) with a view to determining how the purposes or functions of paper-based documents could be fulfilled through electronic-commerce techniques. For example, a paper document may serve any of the following functions: to ensure that a record would be legible by all; to ensure that a record would remain unaltered over time; to allow for the reproduction of a document so that each party would hold a copy of the same data; to allow for the authentication of data by means of a signature; and to provide that a document would be in a form acceptable to public authorities and courts.

6. In respect of all of the above-mentioned functions of paper, electronic records can provide the same level of security as paper and, in most cases, a much higher degree of reliability and speed, especially with respect to the identification of the source and content of the data, provided that a number of technical and legal requirements are met. However, the adoption of the functional-equivalent approach should not result in imposing on users of electronic commerce more stringent standards of security (and the costs associated with them) than in a paper-based environment.

7. The functional-equivalent approach has been taken in article 9 of the Convention with respect to the concepts of "writing", "signature" and "original" but not with respect to other legal concepts dealt with by domestic law. For example, the Convention does not attempt to create a functional equivalent of existing storage requirements, because record storage requirements often serve administrative and regulatory objectives in connection with matters not directly related to the formation or performance of private contracts (such as taxation, monetary regulation, or customs controls). In view of the public policy considerations related to those objectives, and the varying degree of technological development in different countries, it was felt that record storage should be left outside the scope of the Convention.

2. Freedom of form

8. Paragraph 1 reflects the general principle of freedom of form, as stated in article 11 of the United Nations Sales Convention, with a view to making it clear that the reference to possible form requirements under other law does not imply that the Convention itself establishes any form requirement.

9. Nevertheless, the Convention recognizes that form requirements exist and that they may limit the ability of the parties to choose their means of communication. The Convention offers criteria under which electronic communications can meet general form requirements. However, nothing in the Convention implies that the parties have an unlimited right to use the technology or medium of their choice in connection with formation or performance of any type of contract, so as not to interfere with the operation of rules of law that may require, for instance, the use of specific authentication methods in connection with particular types of contract (A/CN.9/571, para. 119).

10. The Convention does not link the validity of an electronic communication or a contract concluded through electronic means to the use of an electronic signature, as most legal systems do not impose a general signature requirement as a condition for the validity of all types of contract (A/CN.9/571, para. 118)

3. Notion of legal requirement

11. In certain common law countries the words "the law" would normally be interpreted as referring to common law rules, as opposed to statutory requirements, while in some civil law jurisdictions the word "the law" is typically used to refer narrowly to legislation enacted by Parliament. In the context of the Convention, however, the words "the law" refer to those various sources of law and are intended to encompass not only statutory or regulatory law, including international conventions or treaties ratified by a Contracting State, but also judicially created law and other procedural law.

12. However, the words "the law" do not include areas of law that have not become part of the law of a State and are sometimes referred to by expressions such as "*lex mercatoria*" or "law merchant" (A/60/17, para. 58). This is a corollary of the principle of party autonomy. To the extent that trade usages and practices develop through industry standards, model contracts and guidelines, it should be left for the drafters and users of those instruments to consider when and under what circumstances electronic communications should be admitted or promoted in the

context of those instruments. Parties who incorporate into their contracts standard industry terms that do not expressly contemplate electronic communications remain free to adapt the standard terms to their concrete needs.

13. Although the article does not refer to the "applicable" law, it is understood, in the light of criteria used to define the geographic field of application of the Convention, that the "law" referred to in this article is the law that applies to the dealings between the parties in accordance with the relevant rules of private international law.

4. Relationship to article 5

14. As indicated above, the principle of party autonomy does not empower the parties to displace legal form requirements by agreeing to use a standard lower than what is provided in article 9 (see A/CN.9/608/Add.1, para. 42). The provisions on general form requirements in the Convention are only facilitative in nature. The consequences of parties using different methods would simply be that they would not be able to meet the form requirements contemplated under article 9 (A/CN.9/548, para. 122).

5. Written form

15. Paragraph 2 defines the basic standard that electronic communications need to meet in order to satisfy a requirement that information be retained or presented "in writing" (or that the information be contained in a "document" or other paper-based instrument).

16. In the preparation of the Convention, UNCITRAL paid attention to the functions traditionally performed by various kinds of "writings" in a paper-based environment. National laws require the use of "writings" for various reasons, such as: (1) to ensure that there would be tangible evidence of the existence and nature of the intent of the parties to bind themselves; (2) to help the parties be aware of the consequences of their entering into a contract; (3) to provide that a document would be legible by all; (4) to provide that a document would remain unaltered over time and provide a permanent record of a transaction; (5) to allow for the reproduction of a document so that each party would hold a copy of the same data; (6) to allow for the authentication of data by means of a signature; (7) to provide that a document would be in a form acceptable to public authorities and courts; (8) to finalize the intent of the author of the "writing" and provide a record of that intent; (9) to allow for the easy storage of data in a tangible form; (10) to facilitate control and subsequent audit for accounting, tax or regulatory purposes; or (11) to bring legal rights and obligations into existence in those cases where a "writing" is required for validity purposes.

17. However, it would be inappropriate to adopt an overly comprehensive notion of the functions performed by a "writing". The requirement of written form is often combined with other concepts distinct from writing, such as signature and original. Thus, the requirement of a "writing" should be considered as the lowest layer in a hierarchy of form requirements, which provides distinct levels of reliability, traceability and integrity with respect to paper documents. The requirement that data be presented in written form (which can be described as a "threshold requirement") should thus not be confused with more stringent requirements such as "signed

writing", "signed original" or "authenticated legal act". For example, under certain national laws, a written document that is neither dated nor signed, and the author of which either is not identified in the written document or is identified by a mere letterhead, would still be regarded as a "writing" although it might be of little evidential weight in the absence of other evidence (e.g. testimony) regarding its authorship. Also, the concept of writing does not necessarily denote inalterability since a "writing" in pencil might still be considered a "writing" under certain existing legal definitions. In general, notions such as "evidence" and "intent of the parties to bind themselves" are to be tied to the more general issues of reliability and authentication of the data and should not be included in the definition of a "writing".

18. The purpose of article 9, paragraph 2, is not to establish a requirement that, in all instances, electronic communications should fulfil all conceivable functions of a writing. Rather than focusing upon specific functions that a "writing" may fulfil in a particular context, article 9 focuses on the basic notion of the information being reproduced and read. That notion is expressed in article 9 in terms that were found to provide an objective criterion, namely that the information in an electronic communication must be accessible so as to be usable for subsequent reference. The use of the word "accessible" is meant to imply that information in the form of computer data should be readable and interpretable, and that the software that might be necessary to render such information readable should be retained. The word "usable" is intended to cover both human use and computer processing. The notion of "subsequent reference" was preferred to notions such as "durability" or "non-alterability", which would have established too harsh standards, and to notions such as "readability" or "intelligibility", which might constitute too subjective criteria.

6. Signature requirements

19. The increased use of electronic authentication techniques as substitutes for handwritten signatures and other traditional authentication procedures has created a need for a specific legal framework to reduce uncertainty as to the legal effect that may result from the use of such modern techniques, to which the Convention generally refers with the expression "electronic signature". The risk that diverging legislative approaches be taken in various countries with respect to electronic signatures calls for uniform legislative provisions to establish the basic rules of what is inherently an international phenomenon, where legal harmony as well as technical interoperability are desirable objectives.

Notion and types of electronic signatures

20. In an electronic environment, the original of a message is indistinguishable from a copy, bears no handwritten signature, and is not on paper. The potential for fraud is considerable, due to the ease of intercepting and altering information in electronic form without detection, and the speed of processing multiple transactions. The purpose of various techniques currently available on the market or still under development is to offer the technical means by which some or all of the functions identified as characteristic of handwritten signatures can be performed in an electronic environment. Such techniques may be referred to broadly as "electronic signatures".

21. In considering uniform rules on electronic signatures, UNCITRAL has examined various electronic signature techniques currently being used or still under development. The common purpose of those techniques is to provide functional equivalents to (a) handwritten signatures; and (b) other kinds of authentication mechanisms used in a paper-based environment (e.g. seals or stamps). The same techniques may perform additional functions in the sphere of electronic commerce, which are derived from the functions of a signature but correspond to no strict equivalent in a paper-based environment.

22. Electronic signatures may take the form of "digital signatures" based on public-key cryptography, and often generated within a "public-key-infrastructure" where the functions of creating and verifying the digital signature are supported by certificates issued by a trusted third party.[1] However, there are various other devices, also covered in the broad notion of "electronic signature", which may currently be used, or considered for future use, with a view to fulfilling one or more of the abovementioned functions of handwritten signatures. For example, certain techniques would rely on authentication through a biometric device based on handwritten signatures. In such a device, the signatory would sign manually, using a special pen, either on a computer screen or on a digital pad. The handwritten signature would then be analyzed by the computer and stored as a set of numerical values, which could be appended to a data message and displayed by the relying party for authentication purposes. Such an authentication system would presuppose that samples of the handwritten signature have been previously analysed and stored by the biometric device. Other techniques would involve the use of personal identification numbers (PINs), digitized versions of handwritten signatures, and other methods, such as clicking an "OK-box".

Technological neutrality

23. Article 9, paragraph 3, is based on the recognition of the functions of a signature in a paper-based environment. In the preparation of the Convention, the following functions of a signature were considered: to identify a person; to provide certainty as to the personal involvement of that person in the act of signing; and to associate that person with the content of a document. It was noted that, in addition, a signature could perform a variety of functions, depending on the nature of the document that is signed. For example, a signature might attest to the intent of a party to be bound by the content of a signed contract, to endorse authorship of a text, to associate itself with the content of a document written by someone else or to show when and at what time a person had been at a given place.

[1] For a detailed description of digital signatures and their applications, see *Guide to Enactment of the UNCITRAL Model Law on Electronic Signatures*, paras. 31-62 (United Nations Sales No. E.02.V.8).

24. Alongside the traditional handwritten signature, there are several procedures (e.g. stamping, perforation), sometimes also referred to as "signatures", that provide varying levels of certainty. For example, some countries generally require that contracts for the sale of goods above a certain amount should be "signed" in order to be enforceable. However, the concept of signature adopted in that context is such that a stamp, perforation or even a typewritten signature or a printed letterhead might be regarded as sufficient to fulfil the signature requirement. At the other end of the spectrum, there are requirements that combine the traditional handwritten signature with additional security procedures such as the confirmation of the signature by witnesses.

25. In theory, it may seem desirable to develop functional equivalents for the various types and levels of signature requirements in existence, so that users would know exactly the degree of legal recognition that could be expected from the use of the various means of authentication. However, any attempt to develop rules on standards and procedures to be used as substitutes for specific instances of "signatures" might create the risk of tying the legal framework provided by the Convention to a given state of technical development.

26. Therefore, the Convention does not attempt to identify specific technological equivalents to particular functions of hand-written signatures. Instead, it establishes the general conditions under which electronic communications would be regarded as authenticated with sufficient credibility and would be enforceable in the face of signature requirements. Focusing on the two basic functions of a signature, subparagraph 3 (a) establishes the principle that, in an electronic environment, the basic legal functions of a signature are performed by way of a method that identifies the originator of an electronic communication, namely to identify the author of a document, and indicates the originator's intention in respect of the information contained in the electronic communication.

27. Given the pace of technological innovation, the Convention provides criteria for the legal recognition of electronic signatures irrespective of the technology used (e.g. digital signatures relying on asymmetric cryptography; biometric devices (enabling the identification of individuals by their physical characteristics, whether by hand or face geometry, fingerprint reading, voice recognition or retina scan, etc.); symmetric cryptography, the use of PINs; the use of "tokens" as a way of authenticating electronic communications through a smart card or other device held by the signatory; digitized versions of handwritten signatures; signature dynamics; and other methods, such as clicking an "OK-box").

Extent of legal recognition

28. The provisions of article 9, paragraph 3, are only intended to remove obstacles to the use of electronic signatures, and do not affect other requirements for the validity of the electronic communication to which the electronic signature relates. Under the Convention, the mere signing of an electronic communication by means of a functional equivalent of a handwritten signature is not intended, in and of itself, to confer legal validity on the electronic communication. Whether an electronic communication that fulfils the requirement of a signature has legal validity is to be settled under the law applicable outside the Convention.

29. For the purposes of paragraph 3, it is irrelevant whether the parties are linked by prior agreement setting forth procedures for electronic communication (such as a trading partner agreement) or whether they had no prior contractual relationship regarding the use of electronic commerce. The Convention is thus intended to provide useful guidance both in a context where national laws would leave the question of authentication of electronic communications entirely to the discretion of the parties and in a context where requirements for signature, which are usually set by mandatory provisions of national law, should not be made subject to alteration by agreement of the parties.

30. The place of origin of an electronic signature, in and of itself, should in no way be a factor determining whether and to what extent foreign certificates or electronic signatures should be recognized as capable of being legally effective in a Contracting State. Determination of whether, or the extent to which, an electronic signature is capable of being legally effective should not depend on the place where the electronic signature was created or where the infrastructure (legal or otherwise) that supports the electronic signature is located, but on its technical reliability.

Basic conditions for functional equivalence

31. According to subparagraph 3 (a), an electronic signature must be capable of identifying the signatory and indicating the signatory's intention in respect of the information contained in the electronic communication.

32. The formulation of subparagraph 3 (b) differs slightly from the wording of article 7, paragraph 1, of the UNCITRAL Model Law on Electronic Commerce, where reference is made to an indication of the signatory's "approval" of the information contained in the electronic communication. It was noted that there might be instances where the law requires a signature, but that signature does not have the function of indicating the signing party's approval of the information contained in the electronic communication. For example, many countries have requirements of law for notarization of a document by a notary or attestation by a commissioner for oath. In such cases, the signature of the notary or commissioner merely identifies the notary or commissioner, and associates the notary or commissioner with the contents of the document, but does not indicate the approval by the notary or commissioner of the information contained in the document. Similarly, some laws require the execution of a document to be witnessed by witnesses, who may be required to append their signatures to that document. The signatures of the witnesses merely identify them and associate them with the contents of the document witnessed, but do not indicate their approval of the information contained in the document (A/60/17, para. 61). The current formulation of subparagraph 3 (a) was agreed upon to make it abundantly clear that the notion of "signature" in the Convention does not necessarily and in all cases imply a party's approval of the entire content of the communication to which the signature is attached (A/60/17, paras. 63-64).

Reliability of signature method

33. Subparagraph 3 (b) establishes a flexible approach to the level of security to be achieved by the method of identification used under subparagraph 3 (a). The method used under subparagraph 3 (a) should be as reliable as is appropriate for the purpose for which the electronic communication is generated or communicated, in

the light of all the circumstances, including any agreement between the originator and the addressee.

34. Legal, technical and commercial factors that may be taken into account in determining whether the method used under subparagraph 3 (a) is appropriate, include the following: (1) the sophistication of the equipment used by each of the parties; (2) the nature of their trade activity; (3) the frequency at which commercial transactions take place between the parties; (4) the kind and size of the transaction; (5) the function of signature requirements in a given statutory and regulatory environment; (6) the capability of communication systems; (7) compliance with authentication procedures set forth by intermediaries; (8) the range of authentication procedures made available by any intermediary; (9) compliance with trade customs and practice; (10) the existence of insurance coverage mechanisms against unauthorized communications; (11) the importance and the value of the information contained in the electronic communication; (12) the availability of alternative methods of identification and the cost of implementation; (13) the degree of acceptance or non-acceptance of the method of identification in the relevant industry or field both at the time the method was agreed upon and the time when the electronic communication was communicated; and (14) any other relevant factor.

35. Subparagraph 3 (b)(i) establishes a "reliability test" with a view to ensuring the correct interpretation of the principle of functional equivalence in respect of electronic signatures. The "reliability test", which appears also in article 7, subparagraph 1 (b), of the UNCITRAL Model Law on Electronic Commerce, reminds courts of the need to take into account factors other than technology, such as the purpose for which the electronic communication was generated or communicated, or a relevant agreement of the parties, in ascertaining whether the electronic signature used was sufficient to identify the signatory. Without subparagraph 3 (b), the courts in some States might be inclined to consider, for instance, that only signature methods that employed high-level security devices are adequate to identify a party, despite an agreement of the parties to use simpler signature methods (A/60/17, paras. 66).

36. However, UNCITRAL considered that the Convention should not allow a party to invoke the "reliability test" to repudiate its signature in cases where the actual identity of the party and its actual intention could be proved (A/60/17, para. 67). The requirement that an electronic signature needs to be "as reliable as appropriate" should not lead a court or trier of fact to invalidate the entire contract on the ground that the electronic signature was not appropriately reliable if there is no dispute about the identity of the person signing or the fact of signing, that is no question as to authenticity of the electronic signature. Such result would be particularly unfortunate, as it would allow a party to a transaction in which a signature was required to try to escape its obligations by denying that its signature (or the other party's signature) was valid—not on the ground that the purported signer did not sign, or that the document it signed had been altered, but only on the ground that the method of signature employed was not "as reliable as appropriate" in the circumstances. In order to avoid these situations, subparagraph 3 (b)(ii) validates a signature method—regardless of its reliability in principle—whenever the method used is proven in fact to have identified the signatory and indicated the signatory's intention in respect of the information contained in the electronic communication (A/60/17, paras. 65-67).

37. The notion of "agreement" in subparagraph 3 (b) is to be interpreted as covering not only bilateral or multilateral agreements concluded between parties directly exchanging electronic communications (e.g. "trading partners agreements", "communication agreements" or " interchange agreements") but also agreements involving intermediaries such as networks (e.g. "third-party service agreements"). Agreements concluded between users of electronic commerce and networks may incorporate "system rules", i.e. administrative and technical rules and procedures to be applied when communicating electronic communications.

7. Electronic originals

38. If "original" were defined as a medium on which information was fixed for the first time, it would be impossible to speak of "original" electronic communications, since the addressee of an electronic communication would always receive a copy thereof. However, paragraphs 4 and 5 should be put in a different context. The notion of "original" in paragraph 4 is useful since in practice many disputes relate to the question of originality of documents, and in electronic commerce the requirement for presentation of originals constitutes one of the main obstacles that the Convention attempts to remove. Although in some jurisdictions the concepts of "writing", "original" and "signature" may overlap, the Convention approaches them as three separate and distinct concepts.

39. Paragraphs 4 and 5 are also useful in clarifying the notions of "writing" and "original", in particular in view of their importance for purposes of evidence. Examples of documents that might require an "original" are trade documents such as weight certificates, agricultural certificates, quality or quantity certificates, inspection reports, insurance certificates, etc. While such documents are not negotiable or used to transfer rights or title, it is essential that they be transmitted unchanged, that is in their "original" form, so that other parties in international commerce may have confidence in their contents. In a paper-based environment, these types of document are usually only accepted if they are "original" to lessen the chance that they be altered, which would be difficult to detect in copies. Various technical means are available to certify the contents of an electronic communication to confirm its "originality". Without this functional equivalent of originality, the sale of goods using electronic commerce would be hampered since the issuers of such documents would be required to retransmit their electronic communication each and every time the goods are sold, or the parties would be forced to use paper documents to supplement the electronic commerce transaction.

40. Paragraphs 4 and 5 should be regarded as stating the minimum acceptable form requirement to be met by an electronic communication for it to be regarded as the functional equivalent of an original. These provisions should be regarded as mandatory, to the same extent that existing provisions regarding the use of paper-based original documents would be regarded as mandatory. The indication that the form requirements stated in paragraphs 4 and 5 are to be regarded as the "minimum acceptable" should not, however, be construed as inviting States to establish requirements stricter than those contained in the Convention by way of declarations made under article 19, paragraph 2.

41. Paragraphs 4 and 5 emphasize the importance of the integrity of the information for its originality and sets out criteria to be taken into account when assessing integrity by reference to systematic recording of the information,

assurance that the information was recorded without lacunae and protection of the data against alteration. It links the concept of originality to a method of authentication and puts the focus on the method of authentication to be followed in order to meet the requirement. It is based on the following elements: a simple criterion as to "integrity" of the data; a description of the elements to be taken into account in assessing the integrity; and an element of flexibility in the form of a reference to the surrounding circumstances. As regards the words "the time when it was first generated in its final form" in subparagraph 5 (a), it should be noted that the provision is intended to encompass the situation where information was first composed as a paper document and subsequently transferred on to a computer. In such a situation, subparagraph 5 (a) is to be interpreted as requiring assurances that the information has remained complete and unaltered from the time when it was composed as a paper document onwards, and not only as from the time when it was translated into electronic form. However, where several drafts were created and stored before the final message was composed, subparagraph 5 (a) should not be misinterpreted as requiring assurance as to the integrity of the drafts.

42. Paragraph 5 sets forth the criteria for assessing integrity, taking care to except necessary additions to the first (or "original") electronic communication such as endorsements, certifications, notarizations, etc. from other alterations. As long as the contents of an electronic communication remain complete and unaltered, necessary additions to that electronic communication would not affect its "originality". Thus when an electronic certificate is added to the end of an "original" electronic communication to attest to the "originality" of that electronic communication, or when data is automatically added by computer systems at the start and the finish of an electronic communication in order to transmit it, such additions would be considered as if they were a supplemental piece of paper with an "original" piece of paper, or the envelope and stamp used to send that "original" piece of paper.

References to preparatory work:

UNCITRAL, 38th session (Vienna, 4-15 July 2005)	A/60/17, paras. 54-76
WG.IV, 44th session (Vienna, 11-22 October 2004)	A/CN.9/571, paras. 123-139
WG.IV, 43rd session (New York, 15-19 March 2004)	
WG.IV, 42nd session (Vienna, 17-21 November 2003)	A/CN.9/546, paras. 46-58
WG.IV, 39th session (New York, 11-15 March 2002)	A/CN.9/509, paras. 112-121

Article 10. Time and place of dispatch and receipt of electronic communications

1. The time of dispatch of an electronic communication is the time when it leaves an information system under the control of the originator or of the party who sent it on behalf of the originator or, if the electronic communication has not left an information system under the control of the originator or of the party who sent it on behalf of the originator, the time when the electronic communication is received.

2. The time of receipt of an electronic communication is the time when it becomes capable of being retrieved by the addressee at an electronic address designated by the addressee. The time of receipt of an electronic communication at another electronic address of the addressee is the time when it becomes capable of being retrieved by the addressee at that address and the addressee becomes aware that the electronic communication has been sent to that address. An electronic communication is presumed to be capable of being retrieved by the addressee when it reaches the addressee's electronic address.

3. An electronic communication is deemed to be dispatched at the place where the originator has its place of business and is deemed to be received at the place where the addressee has its place of business, as determined in accordance with article 6.

4. Paragraph 2 of this article applies notwithstanding that the place where the information system supporting an electronic address is located may be different from the place where the electronic communication is deemed to be received under paragraph 3 of this article.

1. Purpose of the article

43. When the parties deal through more traditional means, the effectiveness of the communications they exchange depends on various factors, including the time of their receipt or dispatch, as appropriate. Although some legal systems have general rules on the effectiveness of communications in a contractual context, in many legal systems general rules are derived from the specific rules that govern the effectiveness of offer and acceptance for purposes of contract formation. The essential question before UNCITRAL was how to formulate rules on time of receipt and dispatch of electronic communications that adequately transpose to the context of the Convention the existing rules for other means of communication.

44. Domestic rules on contract formation often distinguish between "instantaneous" and "non-instantaneous" communications of offer and acceptance or between communications exchanged between parties present at the same place at the same time (*inter praesentes*) or communications exchanged at a distance (*inter absentes*). Typically, unless the parties engage in "instantaneous" communication or are negotiating face-to-face, a contract will be formed when an "offer" to conclude the contract has been expressly or tacitly "accepted" by the party or parties to whom it was addressed.

45. Leaving aside the possibility of contract formation through performance or other actions implying acceptance, which usually involves a finding of facts, the controlling factor for contract formation where the communications are not "instantaneous" is the time when an acceptance of an offer becomes effective. There are currently four main theories for determining when an acceptance becomes effective under general contract law, although they are rarely applied in pure form or for all situations.

46. Pursuant to the "declaration" theory, a contract is formed when the offeree produces some external manifestation of its intent to accept the offer, even though this may not yet be known to the offeror. According to the "mailbox rule", which is traditionally applied in most common law jurisdictions, but also in some countries belonging to the civil law tradition, acceptance of an offer is effective upon dispatch by the offeree (for example, by placing a letter in a mailbox). In turn, under the "reception" theory, which has been adopted in several civil law jurisdictions, the acceptance becomes effective when it reaches the offeror. Lastly, the "information" theory requires knowledge of the acceptance for a contract to be formed. Of all these theories, the "mailbox rule" and the reception theory are the most commonly applied for business transactions

47. In preparing article 10, UNCITRAL recognized that contracts other than sales contracts governed by the rules on contract formation in the United Nations Sales Convention are in most cases not subject to a uniform international regime. Different legal systems use various criteria to establish when a contract is formed and UNCITRAL took the view that it should not attempt to provide a rule on the time of contract formation that might be at variance with the rules on contract formation of the law applicable to any given contract (A/CN.9/528, para. 103; see also A/CN.9/546, paras. 119-121). Instead, the Convention offers guidance that allow for the application, in the context of electronic contracting, of the concepts traditionally used in international conventions and domestic law, such as "dispatch" and "receipt" of communications. To the extent that those traditional concepts are essential for the application of rules on contract formation under domestic and uniform law, UNCITRAL considered that it was very important to provide functionally equivalent concepts for an electronic environment (A/CN.9/528, para. 137)

48. However, article 10, paragraph 2, does not address the efficacy of the electronic communication that is sent or received. Whether a communication is unintelligible or unusable by a recipient is therefore a separate issue from whether that communication was sent or received. The effectiveness of an illegible communication, or whether it binds any party, are questions left to other law.

2. "Dispatch" of electronic communications

49. Paragraph 1 follows in principle the rule set out in article 15 of the UNCITRAL Model Law on Electronic Commerce, although it provides that the time of dispatch is when the electronic communication leaves an information system under the control of the originator rather than the time when the electronic communication enters an information system outside the control of the originator (A/60/17, para. 78). The definition of "dispatch" as the time when an electronic communication left an information system under the control of the originator—as distinct from the time when it entered another information system—was chosen so as to more closely mirror the notion of "dispatch" in a non-electronic environment (A/CN.9/571, para. 142), which is understood in most legal systems as the time when a communication leaves the originator's sphere of control. In practice, the result should be the same as under article 15, paragraph 1, of the UNCITRAL Model Law on Electronic Commerce, since the most easily accessible evidence to prove that a communication has left an information system under the control of the originator is the indication, in the relevant transmission protocol, of the time when

the communication was delivered to the destination information system or to intermediary transmission systems.

50. Article 10 also covers situations where an electronic communication has not left an information system under the control of the originator. This hypothesis, which is not covered in article 12 of the UNCITRAL Model Law on Electronic Commerce, may happen, for example, when the parties exchange communications through the same information system or network, so that the electronic communication never really enters a system under the control of another party. In such cases, dispatch and receipt of the electronic communication coincide.

3. "Receipt" of electronic communications

51. The time of receipt of an electronic communication is the time when it becomes capable of being retrieved by the addressee at an electronic address designated by the addressee. This is presumed to occur when the electronic communication reaches the addressee's electronic address. Paragraph 2 of article 10 is based on a similar rule in article 15, paragraph 2, of the UNCITRAL Model Law on Electronic Commerce, although with a different wording.

"Capable of being retrieved"

52. Paragraph 2 is conceived as a set of presumptions, rather than a firm rule on receipt of electronic communications. Paragraph 2 aims at achieving an equitable allocation of the risk of loss of electronic communications. It takes into account the need to offer the originator an objective default rule to establish whether a message can be seen as having being received or not. At the same time, however, paragraph 2 recognizes that concerns over security of information and communications in the business world had led to the increased use of security measures such as filters or firewalls which might prevent electronic communications from reaching their addressees. Using a notion common to many legal systems, and reflected in domestic enactments of the UNCITRAL Model Law on Electronic Commerce, this paragraph requires that an electronic communication be capable of being retrieved, in order to be deemed to have been received by the addressee. This requirement is not contained in the Model Law, which focuses on timing and defers to national law on whether electronic communications need to meet other requirements (such as "processability") in order to be deemed to have been received.[2]

53. The legal effect of retrieval falls outside the scope of the Convention, and is left for the applicable law. Like article 24 of the United Nations Sales Convention, paragraph 2 is not concerned with national public holidays and customary working hours, elements that would have led to problems and to legal uncertainty in an instrument that applied to international transactions (A/CN.9/571, para. 159).

54. By the same token, the Convention does not intend to overrule provisions of domestic law under which receipt of an electronic communication may occur at the time when the communication enters the sphere of the addressee, irrespective of whether the communication is intelligible or usable by the addressee. Nor is the

[2] See, on this particular point, a comparative study conducted by the Secretariat in A/CN.9/WG.IV/WP.104/Add2, paras. 10-31, available at http://www.uncitral.org/english/workinggroups/wg_ec/wp-104-add2-e.pdf.

Convention intended to run counter to trade usages, under which certain encoded messages are deemed to be received even before they are usable by, or intelligible for, the addressee. It was felt that the Convention should not create a more stringent requirement than currently exists in a paper-based environment, where a message can be considered to be received even if it is not intelligible for the addressee or not intended to be intelligible to the addressee (e.g. where encrypted data is transmitted to a depository for the sole purpose of retention in the context of intellectual property rights protection).

55. Despite the different wording used, the effect of the rules on receipt of electronic communications in the Convention is consistent with article 15 of the UNCITRAL Model Law on Electronic Commerce. As is the case under article 15 of the Model Law, the Convention retains the objective test of entry of a communication in an information system to determine when an electronic communication is presumed to be "capable of being retrieved" and therefore "received". The requirement that an electronic communication should be capable of being retrieved, which is presumed to occur when the communication reaches the addressee's electronic address, should not be seen as adding an extraneous subjective element to the rule contained in article 15 of the Model Law. In fact "entry" in an information system is understood under article 15 of the Model Law as the time when an electronic communication "becomes available for processing within that information system",[3] which is arguably also the time when the communication becomes "capable of being retrieved" by the addressee.

56. Whether or not an electronic communication is indeed "capable of being retrieved" is a factual matter outside the Convention. UNCITRAL took note of the increasing use of security filters (such as "spam" filters) and other technologies restricting the receipt of unwanted or potentially harmful communications (such as communications suspected of containing computer viruses). The presumption that an electronic communication becomes capable of being retrieved by the addressee when it reaches the addressee's electronic address may be rebutted by evidence showing that the addressee had in fact no means of retrieving the communication (A/60/17, para. 80; see also A/CN.9/571, paras. 149 and 160).

"Electronic address"

57. Similar to a number of domestic laws, the Convention uses the term "electronic address", instead of "information system", which was the expression used in the Model Law. In practice, the new terminology, which appears in other international instruments such as the Uniform Customs and Practices for Documentary Credits ("UCP 500")—Supplement for Electronic Presentation ("eUCP"),[4] should not lead to any substantive difference. Indeed, the term "electronic address" may, depending on the technology used, refer to a communications network, and in other instances could include an electronic mailbox, a telecopy device or another specific "portion or location in an information system that a person uses for receiving electronic messages" (A/CN.9/571, para. 157).

---

[3] See *Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce* (United Nations publication, Sales No. E.99.V.4), para. 103.

[4] See James E. Byrne and Dan Taylor, *ICC Guide to the eUCP*, ICC, Paris, 2002, p. 54.

58. The notion of "electronic address", like the notion of "information system", should not be confused with information service providers or telecommunications carriers that might offer intermediary services or technical support infrastructure for the exchange of electronic communications (A/CN.9/528, para. 149).

"Designated" and "non-designated" electronic addresses

59. The Convention retains the distinction made in article 15 of the Model Law between delivery of messages to specifically designated electronic addresses and delivery of messages to an address not specifically designated. In the first case, the rule of receipt is essentially the same as under article 15, paragraph (2)(a)(i), of the Model Law, that is, a message is received when it reaches the addressee's electronic address (or "enters" the addressee's "information system" in the terminology of the Model Law). The Convention does not contain specific provisions as to how the designation of an information system should be made, or whether the addressee could make a change after such a designation.

60. In distinguishing between designated and non-designated electronic addresses, paragraph 2 aims at establishing a fair allocation of risks and responsibilities between originator and addressee. In normal business dealings, parties who own more than one electronic address could be expected to take the care of designating a particular one for the receipt of messages of a certain nature, and to refrain from disseminating, electronic addresses they rarely used for business purposes. By the same token, however, parties should be expected not to address electronic communications containing information of a particular business nature (e.g. acceptance of a contract offer) to an electronic address they knew or ought to have known would not be used to process communications of such a nature (e.g. an e-mail address used to handle consumer complaints). It would not be reasonable to expect that the addressee, in particular large business entities, should pay the same level of attention to all the electronic addresses it owned (A/CN.9/528, para. 145).

61. One noticeable difference between the Convention and the UNCITRAL Model Law on Electronic Commerce, however, concerns the rules for receipt of electronic communications sent to a non-designated address. The Model Law distinguishes between communications sent to an information system other than the designated one and communications sent to any information system of the addressee in the absence of any particular designation. In the first case, the Model Law does not regard the message as being received until the addressee actually retrieves it. The rationale behind this rule is that if the originator chose to ignore the addressee's instructions and sent the electronic communication to an information system other than the designated system, it would not be reasonable to consider the communication as having been delivered to the addressee until the addressee has actually retrieved it. In the second situation, however, the underlying assumption of the Model Law was that for the addressee it was irrelevant to which information system the electronic communication would be sent, in which case it would be reasonable to presume that it would accept electronic communications through any of its information systems.

62. In this particular situation, the Convention follows the approach taken in a number of domestic enactments of the Model Law and treats both situations in the same manner. Thus for all cases where the message is not delivered to a designated electronic address, receipt under the Convention only occurs when (a) the electronic

communication becomes capable of being retrieved by the addressee (by reaching an electronic address of the addressee) and (b) the addressee actually becomes aware that the communication was sent to that particular address.

63. In cases where the addressee has designated an electronic address, but the communication was sent elsewhere, the rule in the Convention is not different in result from article 15, paragraph (2)(a)(ii), of the Model Law, which itself requires, in those cases, that the addressee retrieves the message (which in most cases would be the immediate evidence that the addressee became aware that the electronic communication has been sent to that address).

64. The only substantive difference between the Convention and the Model Law, therefore, concerns the receipt of communications in the absence of any designation. In this particular case, UNCITRAL agreed that practical developments since the adoption of the Model Law justified a departure from the original rule. It also considered, for instance, that many persons have more than one electronic address and could not be reasonably expected to anticipate receiving legally binding communications at all addresses they maintain (A/60/17, para. 82).

Awareness of delivery

65. The addressee's awareness that the electronic communication has been sent to a particular non-designated address is a factual manner that could be proven by objective evidence, such as a record of notice given otherwise to the addressee, or a transmission protocol or other automatic delivery message stating that the electronic communication had been retrieved or displayed at the addressee's computer.

4. Place of dispatch and receipt

66. The purpose of paragraphs 3 and 4 is to deal with the place of receipt of electronic communications. The principal reason for including these rules is to address a characteristic of electronic commerce that may not be treated adequately under existing law, namely, that very often the information system of the addressee where the electronic communication is received, or from which the electronic communication is retrieved, is located in a jurisdiction other than that in which the addressee itself is located. Thus, the rationale behind the provision is to ensure that the location of an information system is not the determinant element, and that there is some reasonable connection between the addressee and what is deemed to be the place of receipt, and that that place can be readily ascertained by the originator.

67. Paragraph 3 contains a firm rule and not merely a presumption. Consistent with its objective of avoiding a duality of regimes for online and offline transactions and, taking the United Nations Sales Convention as a precedent, where the focus was on the actual place of business of the party, the phrase "deemed to be" has been chosen deliberately to avoid attaching legal significance to the use of a server in a particular jurisdiction that differed from the jurisdiction where the place of business was located simply because that was the place where an electronic communication had reached the information system where the addressee's electronic address was located (A/60/17, para. 83).

68. The effect of paragraph 3 therefore is to introduce a distinction between the deemed place of receipt and the place actually reached by an electronic communication at the time of its receipt under paragraph 2. This distinction is not to

be interpreted as apportioning risks between the originator and the addressee in case of damage or loss of an electronic communication between the time of its receipt under paragraph 2 and the time when it reached its place of receipt under paragraph 3. Paragraph 3 establishes a rule on location to be used where another body of law (e.g. on formation of contracts or conflict of laws) requires determination of the place of receipt of an electronic communication.

References to preparatory work:

UNCITRAL, 38th session (Vienna, 4-15 July 2005)	A/60/17, paras. 77-84
WG.IV, 44th session (Vienna, 11-22 October 2004)	A/CN.9/571, paras. 140-166
WG.IV, 42nd session (Vienna, 17-21 November 2003)	A/CN.9/546, paras. 59-86
WG.IV, 41st session (New York, 5-9 May 2003)	A/CN.9/528, paras. 132-151
WG.IV, 39th session (New York, 11-15 March 2002)	A/CN.9/509, paras. 93-98